Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
    - *The database server is highly valuable to the business because it stores all inventory data and information about new products. This information is essential for sales, marketing, and customer engagement.*
- *Why is it important for the business to secure the data on the server?*
    - *Because a hacker or unauthorized actor could easily retrieve sensitive information from the open database and use it maliciously. A competitor could also gain insights into product offerings and strategies, which could harm the business.*
- *How might the server impact the business if it were disabled?*
    - *If the server is disabled, it would slow down operations and reduce customer satisfaction. Customers might be unable to access their accounts or make purchases, leading to frustration and the potential loss of business to competitors.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious Hacker	*Initiate Denial-of-Service (DoS) to disrupt database availability*	*2*	*3*	*6*
Ransomware Attacker	*Temporarily disable database access to demand ransom for restored access*	*1*	*3*	*3*

Approach

This assessment considered the data storage and management methods of the business. The likelihood of a threat occurrence and the potential impact of each event were evaluated in relation to day-to-day operations. There is a high likelihood that a malicious hacker could initiate a DoS attack to disrupt the database, which would significantly impact business continuity. Furthermore, a competitor could now easily observe the company's operations and replicate or undercut its offerings, potentially leading to a loss of customers and revenue. These scenarios represent realistic and significant risks due to the public exposure of the server.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms ensures that only authorized users can access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS (instead of SSL) and IP allow-listing for corporate offices can prevent unauthorized users from accessing the system externally.

To further reduce risk, the organization should enforce the principle of least privilege, ensuring that only necessary users have access to the database. Strict access policies should be implemented to regularly audit and remove inactive or unauthorized users. Limiting access and

continuously monitoring for misuse helps prevent future data leaks and mitigates potential attacks such as ransomware and exfiltration.